Regulating Hate Speech on the Internet:
Unilateralism v Multilateralism,
Technique v Law

Kerem BATIR

Marmara University
European Community Institute
EU Law Dept.

Phone: (216) 336 33 35
Fax: (216) 347 45 43
E-mail: kbatir@hotmail.com

Introduction

Online hate speech is one of the controversial issues of today's cyberspace. First Amendment protection in the US drives the problem through unsolved. But there are attempts of European Governments to regulate hate speech.

According to Lessig, speech divides into three sorts — (1) speech that everyone has a right to (political speech, speech about public affairs); (2)speech that no one has a right to (obscene speech, child porn); and (3)speech that some have a right to but others do not (in the United States, *Ginsberg* speech, or speech that is "harmful to minors," to which adults have a right but kids do not). Speech-protective regimes, on this view, are those where category (1) speech predominates; speech-repressive regimes are those where categories (2) and (3) prevail. And Lessig also adds international dimension to the third category 'speech that is permitted to some in some places, but not to others in other places.' He describes this category by giving examples from Europe. For example Nazi speech constitutes political speech in the United States but it is banned in Germany (Lessig-Resnick: 1998-p.395).

As to be expected, the strongest laws criminalizing hate speech are found in those countries scarred by the Holocaust. In Germany, a number of provisions of the criminal code are directed at expression that is inconsistent with the "dignity of the human personality developing freely within the social community," the fundamental right preserved in the German Constitution. For example, Section 130 of the Criminal Code condemns attacks on human dignity that incite hatred. Section 131 of that same Code proscribes the production or dissemination of hate speech in written form. Section 194 permits prosecution for the denial of the existence of the Holocaust where the disavowal is stated to a person who is a member of a group persecuted by the Nazi regime. Section 86 forbids the distribution of propaganda that promotes (1) the precepts of the Nazi regime, (2) unconstitutional parties, or (3) prohibited associations. And Section 86a censures the use of insignia--including flags, uniforms, badges and salutes--of these same proscribed organizations (Mayer-Schönberger, Teree Foster,1997).

In this article I will try to examine the possible ways to regulate hate speech. I also discuss the model developed by Lawrence Lessig and Paul Resnick 'Mandated Access Control' as a method of regulating hate speech. As a starting point Licra v. Yahoo case is

very useful to show us how a national court's decision has effects outside its jurisdiction. It also shows us the weakness of unilateral actions to regulate online hate.

There are four possible ways achieving the target of protecting society from illegal and harmful content

1. Unilateral actions of States
2. International Agreements on content regulation
3. Self-regulatory systems
4. Mandated access controls

Because of the concept of the essay, I will not discuss self-regulatory systems in detail.

Unilateral Actions of States for Regulating the Online Hate Content

France : LICRA v. Yahoo France Case

The League against Racism and Anti-Semitism (LICRA) brought an action against Yahoo France in May 2000. They argued that Yahoo! Inc hosted an auction site, which held thousands of Nazi objects for sale. Yahoo France provided links from its website to that auction site. According to French law it is an offence to the 'collective memory' of the country and simply displaying those symbols (uniforms worn by German soldiers, emblems etc.) thus such an action constitutes violence of Penal Code.

The French court, in 22 May 2000, ordered Yahoo! Inc to take all necessary measures to make impossible to access this auction site and other sites containing Nazism from France. And also ordered Yahoo France to place a warning informing them to risks involved in continuing to view such sites.

Yahoo argued that the services were given by an US firm (Yahoo inc) in the United States. There is no jurisdiction for French Courts and Court of Paris is not the competent body to make a ruling in that dispute. Yahoo also argued that because its servers were located in the USA First Amendment of the US Constitution protected its freedom of speech rights.

A panel of experts appointed by the court in order to find a possible solution. Experts discussed the possibility of differentiation of French surfers to others. They came to a conclusion that it was possible to distinguish 70% of the French users by their IP addresses. The rest were using international ISP's and because of the dynamic IP numbers it was impossible to guess. The experts also advised to the court that ISPs should require surfers that are not identified by IP address to declare nationality before entering the auction site. The ability of nationality identification was evidenced by Yahoo banner adds, which displayed in French for French surfers.

In response Yahoo placed a warning notice in such categories (e.g. holocaust) to surfers who search by tree structure. But this notice did not satisfy the French court. In November 2000 the Paris court rejected the plea of incompetence and ordered Yahoo Inc. to comply with the order within three months as of the notification along with the injunctions contained in the order of 22 May 2000 subject to a penalty of 100,000 francs per day of delay effective from the first day following the expiration of 3 months period.

Subsequent to the decision Yahoo inc. declared that they would no longer allow Nazi and Ku Klux Klan memorabilia to display on its websites and a more proactive approach with a monitoring and filtering system would be running. Yahoo also asked US District Court (San Jose) to declare that French ruling is unconstitutional under US constitution and French courts had no jurisdiction over the content produced by the US firms. At the end the motion for summary judgement was granted and French judgement had no value within US jurisdiction.

United States

The first amendment of the US constitution provides the most powerful protection for the freedom of speech. Any attempt by a governmental entity to restrict speech on the basis of its hateful content would be deemed content-based regulation, a type of regulation that is disfavoured and presumed unconstitutional under first amendment Law.

Speech can be regulated on the basis of its content if it is found to be: obscene, child pornography, fighting words, incitement to immanent lawless conduct, defamation (libel or slander), an invasion of privacy under tort law, harassment, copyright infringement or another recognized tort or crime.

There is no content-based exception for hate related speech per se, it must be shown that the expressive activity in a particular situation falls within one or more of the ten exceptions written above.

Stuart Biegel examined all the exemptions and came to conclusion that under current U.S. First Amendment Law, extremist and hate-related websites cannot generally be restricted. The other typical form of online hate (e-mails or chat rooms) is arguable similar in nature to phone conversation. Unless it constitutes harassment at individual level, it is not possible to bring to court what is said. As a conclusion basic online hate is legal in the US and cannot be limited (Biegel, 2001:p.344)

The Spillover Effect of Unilateral Regulations:

CompuServe Case (Germany)

CompuServe Deutschland was a 100% subsidiary of CompuServe USA. It provided dial-up access to CompuServe USA's content and Internet services. At the end of 1995 German police warned the firm that the Usenet newsgroups in the system contained images of violence, child pornography and bestiality. This content was stored on CompuServe USA's newsgroup servers. The parent company blocked access to those newsgroups worldwide and provided parental control software to users and than unblocked the access. But according to German law giving access to adults to the incriminated content was illegal. On May 1998, the director of CompuServe Deutschland was sentenced two-year imprisonment.

This case is related to child pornography but response from sector was very important. The leading European ISP's came together and under Bertelsmann Foundation umbrella they formed a statement of principles for self-regulation of Internet content. They stressed on self-regulation must be supported by public authorities and the need for codes of conduct to be adopted to ensure that internet content and service providers act in accordance with principles of social responsibility (Grainger,2000: p.92)

CompuServe case is a good example for spillover effects of national jurisdiction. At the time CompuServe was not able to control geographical flow of the information on discussion groups and Munich court judgement had the effect of blocking access to these discussion groups for all users around the world.

Yahoo France case had fewer implications in international area. Yahoo ended auctioning of Nazi and Ku Klux Klan memorabilia on its website but did not take further steps which were required by French Court. It would not interfere with non-commercial material in chat rooms. It was issued a monitoring system but Yahoo Officials asserted that 'had nothing to do with the actions of Judge Gomez, but rather were part of a general housecleaning of its auction policy and the result of ongoing discussions with Jewish groups in the United States (Penfold, 2001)

The solution for a global Internet company is to conform its activities to the most restrictive national regulation. This will broaden the content on Internet and limit liberties of other nations.

According to Jack Goldsmith unilateral national regulation of harmful local effects of Internet information flow is perfectly legitimate. And his conclusion is not affected by the presence of spill over effects (Goldsmith, 2000- p.143). He gave the example of Boeing-McDonnell merger. Boeing and McDonnell are two US firms doing business worldwide. The US Competition authority FTC investigated and approved this merger. But European Commission was very sensitive on the subject. Boeing had contractual relations with major airlines and this merger threatened European competition such as Airbus. The two companies had two choices: 1. Merge and stop doing business in Europe, 2.Continue doing business in Europe and comply with the European regulation. The companies decided to choose the second one as they had a considerable business in Europe.

Goldsmith argues that for foreign companies like CompuServe, the German regulation is a cost of doing business in Germany. In the absence of some substantive international law to the contrary, Germany can regulate the local harm of transnational internet activity even if this regulation produces spill over effects (Goldsmith, 2001:p.145).

There are responses to Goldsmith's arguments (Benkler,2000:p.178). Multinational companies do business all over the world. They do business in Germany but in China too. If CompuServe or any other company is forced to allow content that Chinese democracy prohibits then what will be the future of the Internet?

International Agreements on content regulation

There have been several attempts made for regulating content in international area. In European level DG XIII (responsible for telecommunications) took the initiative in respect of harmful content on the Internet. On 26 November 1997 Action plan on Promoting the Safe use of the Internet was announced by European Commission. These guidelines were built on the self-regulatory approach developing in the UK and some other EU member states. The key principles of this action plan were (com (97) page 582):

- Promotion of self-regulation and creation of content-monitoring schemes including a European network of hotlines to achieve a high level of protection (especially dealing with content such as child pornography and racism);
- Demonstration and application of effective filtering services and compatible rating systems, which take account of cultural and linguistic diversity; and
- Promotion of awareness actions directed at users to allow them to use Internet resources provided by industry safely and with confidence.

The action plan also identified that illegal content must be distinguished from harmful content. Illegal content must be dealt with at source by law enforcement agencies, and that there activities are covered by the rules of national law and agreements of judicial cooperation. But industry should give importance to help reducing the circulation of illegal content through properly functioning systems of self-regulation. Child pornography, racism and anti-Semitism were counted as illegal content by the commission. In harmful content area priority was given to self-control mechanisms.

The organization for Economic Cooperation and Development (OECD)
Belgium, after the events occurred in 1996, put some pressure for online content regulation within OECD. This action was strongly supported by France. But there was a huge divergence of view between these countries and United States. OECD resolved this problem by taking no further action.

There were some other attempts by various international organizations such as UNESCO, the Global Business Dialogue, the International Network of Experts on Internet Content but all these activities were focused on self-regulation issues e.g. filtering technologies, content rating.

More recently Council of Europe has taken the initiative in content regulation. The Convention on Cybercrime was signed by 31 states on 23 November 2001 including United States, Canada, Japan and South Africa. This Convention will enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe (art.36/3). There is no ratification till today (9 April 2002). Council of Europe (CoE) is a regional intergovernmental organization with 43 member countries. The Convention is open to signature by member states and non-member states. Title 3 under Section 1 is dealt with Content Regulation. Article 9 listed criminal offences related to child pornography. There is no provision related to hate speech in original convention but CoE is willing to take further steps in content regulation.

Committee Of Experts On The Criminalisation Of Acts Of A Racist Or Xenophobic Nature Committed Through Computer Systems drafted First Additional Protocol to the Convention on cybercrime. This Additional protocol explicitly drafted for the criminalisation of acts of a racist or xenophobic nature committed through computer systems. According to drafted article 1.a “Racist or xenophobic material” is described as; any written material, any image or any other representation of thoughts or theories, which advocates, promotes r incites hatred, discrimination or violence against any individual or group of individuals, based on race, color, [religion, descent, nationality,] national or ethnic origin”. This draft protocol is open to all parties, which ratified the Cybercrime convention.

Mandated Access Controls:

Lawrence Lessig and Paul Resnick proposed this model in their article. First the writers tried to understand the problem. There are nearly 200 countries all over the world. Each of them has different traditions, cultures and values. It is very difficult to regulate the content through the needs of all international community. If we try to tailor a dress according to all needs at the end it will not suit anybody. So the model ‘mandated access control’ can provide the possible solution. There are three types of actors in online world. These are: senders, intermediaries and recipients. In present situation senders act equally to all recipients regardless of their jurisdiction and recipients don’t care about the items that they want from the sender whether they are illegal in their country or not. And intermediaries act neutrally while transactions were taken place. The solution lies here. If

the senders be given more information about recipient's jurisdiction and type, this can be done by requiring certificates or database mapping IP addresses to jurisdictions, and if the recipients be given more information about items, this can be done by providing labels and government lists of what is permitted and what is prohibited then the senders will not realized the transactions which will be illegal in that jurisdiction.

The expert reports in Licra v. Yahoo case showed us that it is possible to distinguish the Internet users according to their IP numbers. 70% of users in France have specific IP numbers that can be distinguishable among others. And Yahoo placed adds in French for its French consumers that supported the idea yahoo is able to know who is French on its system.

This system will give greater control of content to National Governments. And ISPs will gain the power to regulate the behavior on the Net. ISPs, as intermediaries, will monitor the activities on Internet and use proxies and application gateways in order to secure national jurisdiction will create 'Big Brother' in George Orwell's novel 1984.

According to Reporters Without Borders website 59 countries have some bad records in Internet governance. They used technical means to control access in several ways:

1. No Internet no worries: Countries like North Korea, Iraq and Libya completely restricted access to the Internet.
2. Monopoly + Filter: Countries like Belarus and Sudan controlled the servers and filtered the websites outside.
3. Hardware control: China acted legislation that each computer connected to Internet must obtain registration from government.

I totally agree with Lessig's argument but we have to see the problems of today's Internet world and if we built a new system which will give more power to both service providers and national governments the result will not be a free world.

The problem of technology-based solutions is they can be challenged by technology-based attacks. There will be programs like anomymizer, which provide ability of disguising IP number, and other possible solutions for reaching the illegal content that

users want. But these users are less in number and majority will be under control of national jurisdiction.

Conclusion

Regulating the child pornography is the first step for content regulation. It is also the easiest step too. All states agreed on the illegality of the subject. As an illegal activity enforcement measures can be taken easily. Child pornography falls outside the US First Amendment protection.

Hate speech is an issue that relates to culture, tradition and history. If you live in homogenous country that 99% of population belongs to same race, religion and ethnic background than Xenophobia may not be a problem for you. Or if you live in a country in which the common belief is that Jews are not good then your government may not take any actions to regulate Anti-Semitism on the Internet.

If we believe that Internet is a borderless place and surfers constitute the Internet society then this society should depend on common values and regulated by common rules. Arguing that each state shall enforce its own rules over Internet will cause fragmentation of the Internet. So there will be no single cyberspace but cyberspaces. Today Chinese human rights activists use Internet to advocate for their cause, Uzbek opposition has only websites to express their opinions to the public. There are several critics of Iranian regime in discussion groups. If we lower the democracy and liberty standards for covering the restrictions of all countries, then Internet will become Disneyland. No political debates, no criticism, no democracy is not the nature of the Internet.

Self-regulatory systems are useful if you have a child to protect him or her from harmful content. But as German court argued in CompuServe the protection is not for children but for all. So who sets self-regulatory systems? Do you want to install cyber-nanny to protect yourself from such illegal or harmful sites?

Lessig's model also carries the risks of misuse. His model allows ISP's and other intermediaters to monitor activities of surfers. If a recipient ordered some material that is forbidden in that territory ISP's have a right to block this transaction (speech). In Iran internet users can't receive e-mails containing words such as freedom or sex (the

enemies of the internet report). The government's telecom monitors the e-mails and deletes the messages containing these silly words. Can this be an example of Lessig's model? Lessig's approach is pragmatic. He knows that US Congress is bound by First amendment law and he does not care the rest of the world.

International agreements cannot be ratified by US Congress because of the first amendment law. But this protection developed by courts decisions. If US Courts forced to take decisions against hate speech then this protection will loose its importance. The main stream is prohibition of hate speech and only USA is out of sight.

Unilateral actions seem to be meaningless but they showed the willingness of states to enforce their laws in cyberspace.

Bibliography

Akdeniz, Yaman, Case Analysis of (the Yahoo case) *League Against Racism and Anti-Semitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France*, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November 2000. [2001] Electronic Business Law Reports, 1(3) pp.110-120. <http://www.cyber-rights.org/documents/yahoo_ya.pdf>

Biegel, Stuart, Beyond Our Control, MIT Pess,2001.

Benkler, Yochai, "Internet regulation: A Case Study in the Problem of Unilateralism", EJIL (2000), Vol.11 No.1, pp.171-185.

Council of Europe, Convention on Cybercrime, 23.11.2001.

<http://conventions.coe.int/treaty/EN/cadreprincipal.htm>

Council of Europe, European Committee On Crime Problems (Cdpc), DRAFT of the First Additional Protocol to the Convention on cybercrime concerning the criminalisation of acts of a racist or xenophobic nature committed through computer systems, 18 - 20 March 2002 <http://www.coe.int/T/E/Legal%5FAffairs/Legal%5Fco%2Doperation/Combating%5Feconomic%5Fcrime/Cybercrime/Racism_on_internet/AP_Protocol (2002) 5E-1.pdf>

EC Commission, Final Action Plan on Promoting the Safe Use of the Internet, 26 November 1997, Com (97), p.582.

Goldsmith, Jack, "Unilateral Regulation of the Internet: A Modest Defence", EJIL (2000), Vol. 11 No.1, pp.135-148.

Grainger, Gareth, "Freedom of expression and regulation of Information in Cyberspace: Issues concerning Potential International Cooperation Principles", in The International Dimensions of Cyberspace Law, edited by Teressa Fuentes-Camacho, UNESCO Publishing, 2000, pp.71-126.

Lessig, Lawrence and Paul Resnick, “Zoning Speech on the Internet: A Legal and Technical Model”, Michigan Law Review, Vol.98 No.2, November 1999,pp. 395-431.

LICRA And UEJF Vs. Yahoo! Inc. And Yahoo France, Order Of November 20, 2000 By The Superior Court Of Paris, Unofficial English Translation <http://www.gigalaw.com/library/france-yahoo-2000-11-20-lapres.html>

Mayer, Franz C., “Europe and the Internet: The Old World and the New Medium”, EJIL (2000), Vol.11 No.1, pp.149-169.

Mayer-Schönberger, Viktor, Teree Foster, “A Regulatory Web: Free Speech and the Global Information Infrastructure”, 3 Mich.Telecomm.Tech.L.Rev. 45 (1997), <http://www.mttlr.org/volthree/foster.html>

Penfold, Carolyn, “Nazis, Porn and Politics: Asserting Control Over Internet Content”, 2001 (2) *The Journal of Information, Law and Technology (JILT)*. <http://elj.warwick.ac.uk/jilt/01-2/penfold.html>

Reporters without borders, The Enemies ofthe Internet Report <http://www.rsf.fr/rsf/uk/>

Steinhardt, Barry, “ Hate Speech” in Akdeniz, Walker and Wall, The Internet, Law and Society, Longman, 2000.

Strossen, Nadine, Cybercrimes V. Cyberliberties, International Review Of Law Computers &Technology, Volume 14, No. 1, 2000, pp. 11–24

Vick, Douglas W., “The Internet’s “Threat” to State Sovereignty: A Case Study” in Morris, Nancy and Silvio Waisbord, Media and Globalization: Why the State Matters, City: Rowman and Littlefield, 2001.

Volokh, Eugene, “Freedom of Speech, Cyberspace, And Harassment Law”, 2001 Stan. Tech. L. Rev. 3

<http://stlr.stanford.edu/STLR/Article/01_STLR_3>

Yahoo v. LICRA Order Granting Motion for Summary Judgement, *United States District Court for the Northern District of California, San Jose Division*
<http://www.cdt.org/jurisdiction/011107judgement.pdf>

Zekos G I, 'Internet or Electronic Technology: A Threat to State Sovereignty', 1999 (3) The Journal of Information, Law and Technology (JILT).
<http://www.law.warwick.ac.uk/jilt/99-3/zekos.html>